

# NETMANAGEIT

## Intelligence Report

### Update: CVE-2024-4577 quickly weaponized to distribute Ransomware



# Table of contents

---

## Overview

● Description	4
● Confidence	4
● Content	5

---

## Entities

● Attack-Pattern	6
● Indicator	15
● Malware	17
● targets	18
● uses	22
● indicates	23
● based-on	27

---

## Observables

---

● Cryptocurrency-Wallet	28
● StixFile	29
● IPv4-Addr	30

---

## External References

---

● External References	31
-----------------------	----

# Overview

## Description

The report describes an attack campaign leveraging the CVE-2024-4577 vulnerability to deliver the "TellYouThePass" ransomware. The attackers use the vulnerability to execute arbitrary PHP code and run a malicious HTML application that loads a .NET variant of the ransomware into memory. Upon execution, the ransomware contacts a command-and-control server, enumerates directories, terminates processes, encrypts files, and leaves a ransom note.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

100 / 100

# Content

N/A

# Attack-Pattern

**Name**

T1497

**ID**

T1497

**Description**

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](<https://attack.mitre.org/techniques/T1497>) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](<https://attack.mitre.org/techniques/T1497>) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

**Name**

T1489

**ID**

T1489

**Description**

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster)

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](<https://attack.mitre.org/techniques/T1485>) or [Data Encrypted for Impact](<https://attack.mitre.org/techniques/T1486>) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

**Name**

T1059.001

**ID**

T1059.001

**Description**

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number

of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

**Name**

T1204.002

**ID**

T1204.002

**Description**

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

**Name**

T1486



**ID**

T1486

**Description**

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](<https://attack.mitre.org/techniques/T1078>), [OS Credential Dumping](<https://attack.mitre.org/techniques/T1003>), and [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](<https://attack.mitre.org/techniques/T1491/001>), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted. (Citation: Rhino S3 Ransomware Part 1)

**Name**

T1059.003

**ID**

T1059.003

**Description**

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

**Name**

T1027

**ID**

T1027

**Description**

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or

archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](<https://attack.mitre.org/techniques/T1027/010>) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](<https://attack.mitre.org/techniques/T1059>). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

**Name**

T1567.002

**ID**

T1567.002

**Description**

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet. Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

**Name**

T1059.005

**ID**

T1059.005

**Description**

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](<https://attack.mitre.org/techniques/T1559/001>) and the [Native API](<https://attack.mitre.org/techniques/T1106>) through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft) Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA) (Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support). (Citation: Microsoft VBScript) Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with VBScript or embedding VBA content into [Spearphishing Attachment](<https://attack.mitre.org/techniques/T1566/001>) payloads (which may also involve [Mark-of-the-Web Bypass](<https://attack.mitre.org/techniques/T1553/005>) to enable execution).(Citation: Default VBS macros Blocking )

**Name**

T1547.001

**ID**

T1547.001

**Description**

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level. The following run keys are created by default on Windows systems: \*

```
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` *
```

```
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` *
```

```
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` *
```

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` Run keys may exist under multiple hives. (Citation: Microsoft Wow6432Node 2018) (Citation: Malwarebytes Wow6432Node 2016) The

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. (Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx:

```

reg add
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.].dll"
  
```

(Citation: Oddvar Moe RunOnceEx Mar 2018) Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`. The following Registry keys can be used to set startup folder items for persistence:

The following Registry keys can be used to set startup folder items for persistence:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` The following Registry keys can control automatic startup of services during boot:

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`

`HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices`

`HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices` Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`

`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` Programs listed in the load value of the registry key

`HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows` run automatically for the currently logged-on user. By default, the multistring `BootExecute` value of the registry key

`HKLM\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot. Adversaries can use these configuration locations to execute malware, such as

remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

**Name**

T1083

**ID**

T1083

**Description**

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`. (Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvr`). (Citation: US-CERT-TA18-106A)

# Indicator

**Name**

9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53']

**Name**

95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3

**Pattern Type**

stix

**Pattern**

[file:hashes!'SHA-256' =  
'95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3']

**Name**

bc1qnuxx83nd4keeeegrumtnu8kup8g02yzgff6z53l

**Pattern Type**

stix

**Pattern**

[cryptocurrency-wallet:value = 'bc1qnuxx83nd4keeeegrumtnu8kup8g02yzgff6z53l']

**Name**

88.218.76.13

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '88.218.76.13']

**Name**

5a2b9ddddea96f21d905036761ab27627bd6db4f5973b006f1e39d4acb04a618

**Pattern Type**

stix

**Pattern**

[file:hashes:'SHA-256' =  
'5a2b9ddddea96f21d905036761ab27627bd6db4f5973b006f1e39d4acb04a618']



# Malware

**Name**

ransomware

**Name**

TellYouThePass

# targets

<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>

# uses

<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>

# indicates

<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>
<b>Name</b>

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**



**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

**Name**

TLP:CLEAR



# based-on

<b>Name</b>
<b>Name</b>
<b>Name</b>

# Cryptocurrency-Wallet

## Value

bc1qnuxx83nd4keeeegrmtnu8kup8g02yzgff6z53l

# StixFile

## Value

9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53

5a2b9ddddea96f21d905036761ab27627bd6db4f5973b006f1e39d4acb04a618

95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3

# IPv4-Addr

## Value

88.218.76.13

# External References

- 
- <https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware>
- 
- <https://otx.alienvault.com/pulse/666823317d16a2e82515f9ca>